UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/576,598	05/22/2000	Solomon W. Golomb	06666-032001	1702

20985 7590 03/30/2004

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER	
ORTIZ, BELIX M	

ART UNIT	PAPER NUMBER
2175	6

DATE MAILED: 03/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PRG

Office Action Summary	Application No. 09/576,598	Applicant(s) GOLOMB ET AL.	
	Examiner Belix M. Ortiz	Art Unit 2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-34 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-34 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. Headings appear underlined and some of them bold and also in lower case throughout the disclosed specification.

   Heading should not be underlined or in bold type and should be in uppercase letters.

2. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(h) DETAILED DESCRIPTION OF THE INVENTION.

(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 4, 11, 22, and 34 are rejected under 35 U.S.C. 102(b) as being anticipated by Seheidt et al. (U.S. patent 5,787,173).

As to claim 1, Seheidt et al. teaches a cryptography method (see abstract), comprising:

determining information to be encrypted (see column 1, lines 12-15; column 1, lines 45-51); and

encrypting the information using an arithmetic which is not associative (see column 4, lines 55-67).

As to claim 4, Seheidt et al. teaches wherein the encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using the first result, and encryption can be iterated an arbitrary number of times (see column 9, lines 32-39).

As to claim 11, Seheidt et al. teaches wherein the first and second encryption form iterative encipherment (see column 9, lines 32-39).

As to claim 22, Seheidt et al. teaches wherein the encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using the first result (see column 9, lines 32-39).

As to claim 34, Seheidt et al. teaches A method of encrypting in a computer (see figure 1), comprising:

obtaining, in the computer, a file to be encrypted (see column 1, lines 12-15; column 1, lines 45-51);

using a non-associative arithmetic to encrypt the file (see column 4, lines 55-67); and

using another non-associative arithmetic to further encrypt the once-encrypted file (see column 4, lines 55-67).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-3, 5-6, 8-9, 14-16, and 19-21 are rejected under 35 U.S.C.103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Scheidt et al. (U.S. patent 6,266,417).

As to claim 2, Seheidt et al. '173 does not teach wherein the encrypting comprises using a non-trivial ci-quasigroup to encode.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches wherein the encrypting comprises using a non-trivial ci-quasigroup to encode (see column 2, lines 46-53).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, to include wherein the encrypting comprises using a non-trivial ci-quasigroup to encode.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173

by the teaching of Scheidt et al. '417, because wherein the encrypting comprises using a non-trivial ci-quasigroup to encode, would enable the cryptography method since the non-trivial ci-quasigroup excludes the use of groups, the quasigroup that are not groups are more efficient and more secure than those based on group. The result of the message would be more difficult to decode by unauthorized receiver.

As to claim 3, Seheidt et al. '173 as modified teaches a method further comprising decoding sing the crossed-inverse function of the ci-quasigroup (see Scheidt et al. '417, column 2, lines 53-61).

As to claim 5, Seheidt et al. '173 as modified teaches a method further comprising defining a rule indicative of the quasigroup (see Scheidt et al. '417, column 4, lines 35-37).

As to claim 6, Seheidt et al. '173 as modified teaches a method further comprising defining a rule indicative of the crossed inverse of the quasigroup (see Scheidt et al. '417, column 4, lines 21-34).

As to claim 8, Seheidt et al. '173 does not teach wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode (see column 2, lines 46-53).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, to include wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 by the teaching of Scheidt et al. '417, because wherein the encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode, would enable the cryptography method since the non-trivial ci-quasigroup excludes the use of groups, the quasigroup that are not groups are more efficient and more secure than those based on group. The result of the message would be more difficult to decode by unauthorized receiver.

As to claim 9, Seheidt et al. '173 as modified teaches a method further comprising distributing information indicative of the quasigroup as a public key, and keeping secret the crossed inverse quasigroup (see Seheidt et al. '173, column 3, lines 4-31).

As to claim 14, Seheidt et al. '173 does not teach wherein the encrypting is carried out using block ciphers.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches wherein the encrypting is carried out using block ciphers (see column 9, lines 23-25).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, to include wherein the encrypting is carried out using block ciphers.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 by the teaching of Scheidt et al. '417, because wherein the encrypting is carried out using block ciphers, would enable the cryptography method because; the security of the block cipher mode is based on the security of the text/key relation and the cryptanalytic resistant mixing properties of an iterated non-linear feedback function. The text/key relation is a symbol permutation consisting of the product of N randomly selected permutations, which are selected from a set of M permutations, which in turn are selected from the full set of W! permutations on W elements. The N permutations change according to a deterministic, but unknown, rule with each application of the function. Thus, even if the same symbol were presented to the text/key relation at two different rounds within the processing of a single block, the permutation applied to that symbol would be the same only with

a probability of 1/W. This maximizes the uncertainty across the total number of rounds of the block cipher (see Scheidt et al. '417, column 9, lines 28-42).

As to claim 15, Seheidt et al. '173 as modified teaches wherein the block cipher are defined by a function (see Scheidt et al. '417, column 9, lines 28-31).

As to claim 16, Seheidt et al. '173 as modified teaches wherein the block ciphers are formed using cross inversed quasigroups, used according to C = f *(M, K)* for the encryption and M=finv *(C,K)* for the decryption (see Scheidt et al. '417, column 8, lines 50-56; column 9, lines 16-27).

As to claim 19, Seheidt et al. '173 teaches a cryptography method, comprising:

encrypting the information using an arithmetic which is not commutative (see column 4, 55-67).

Seheidt et al. '173 does not teach determining information to be encrypted.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches determining information to be encrypted (see column 1, lines 9-12).

Therefore, it would have been obvious to a person having ordinary

skill in the art at the time the invention was made to have modified Seheidt et al. '173, to include determining information to be encrypted.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 by the teaching of Scheidt et al. '417, because determining information to be encrypted, would enable the cryptography method to know what information the user wants to be secure or the information that the user does not want to be seen by unauthorized person.

As to claim 20, Seheidt et al. '173 as modified teaches wherein the encrypting comprises using a quasigroup to encode (see Scheidt et al. '417, column 2, lines 46-53).

As to claim 21, Seheidt et al. '173 as modified teaches a method further comprising decoding using a crossed inverse of the quasigroup (see Scheidt et al. '417, column 2, lines 53-61).

7. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Schweitzer et al. (U.S. patent 5,850,450).

As to claim 7, Seheidt et al. '173 does not teach a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic.

Schweitzer et al., teaches method and apparatus for encryption key creation (see abstract), in which he teaches a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic (see column 5, lines 49-61).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, to include a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 by the teaching of Schweitzer et al., because a method further comprising carrying out a second encrypting using the arithmetic, and wherein a result of the second arithmetic is encrypted exponentially more than a result of the first arithmetic, would enable the cryptography method since exponentiation calculation, according to other characteristics and advantages, speed up the time required for performing a encryption.

8. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Scheidt et al. (U.S. patent 6,266,417) as applied in claims 2-3, 5-6, 8, 14-16, and 19-21 above, and further in view of Hellman et al. (U.S. patent 4,424,414).

As to claim 10, Seheidt et al. '173 as modified still, does not teach wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10}.

Hellman et al., teaches exponentiation cryptographic apparatus and method (see abstract), in which he teaches wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10} (see column 6, lines 19-24).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, as modified, to include wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10}.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 as modified, by the teaching of Hellman et al., because wherein the quasigroup is formed by an n by n square, where n is greater than 10^{10}, would enable the cryptography method because the quasigroup is a set of objects with a multiplication table described by a latin square of size n x n and if n is smallest of 10^{10} the radio of the quasigroup will be infinity.

9. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Hellman et al. (U.S. patent 4,424,414).

As to claim 12, Seheidt et al. does not teach wherein the first interiation is carried out in a different direction than the first encryption.

Hellman et al., teaches exponentiation cryptographic apparatus and method (see abstract), in which he teaches wherein the first interiation is carried out in a different direction than the first encryption (see column 4, lines 53-64).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include wherein the first interiation is carried out in a different direction than the first encryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Hellman et al., because wherein the first interiation is carried out in a different direction than the first encryption, would enable the cryptography method to make on the second encryption, the inverse- quasigroup.

As to claim 13, Seheidt et al. as modified teaches wherein the first direction is left to right and the second direction is right to left (see Hellman et al., column 4, lines 62-64).

10. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Reeds, III (U.S. patent 5,724,427).

As to claim 17, Seheidt et al. does not teach wherein the encrypting uses XIP neofields.

Reeds, III, teaches method and apparatus for autokey rotor encryption (see abstract), in which he teaches wherein the encrypting uses XIP neofields (see column 8, lines 36-50).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include wherein the encrypting uses XIP neofields.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Reeds, III, because wherein the encrypting uses XIP neofields, would enable the cryptography method, since this method of encryption is more elaborate that means that is more secure.

11. Claims 18, 23-26, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Anshel et al. (U.S. patent 5,440,640).

As to claim 18, Seheidt et al. does not teach wherein the encrypting uses near rings.

Anshel et al., teaches multistream encryption system for secure communication (see abstract), in which he teaches wherein the encrypting uses near rings (see column 1, lines 31-35; column 7, line 16).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include wherein the encrypting uses near rings.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Anshel et al., because wherein the encrypting uses near rings, would enable the cryptography method since not all field can be a ring but with the use of near ring just one of the two distributive rules is required.

As to claim 23, Seheidt et al. teaches a cryptography method comprising encrypting information using an arithmetic with an algebraic structure (see column 4, lines 55-67).

Seheidt et al. does not teach the algebraic structure being a nongroup, nonfield structure.

Anshel et al., teaches multistream encryption system for secure communication (see abstract), in which he teaches the algebraic structure being a nongroup, nonfield structure (see abstract).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al., to include the algebraic structure being a nongroup, nonfield structure.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. by the teaching of Anshel et al., because the algebraic structure being a nongroup, nonfield structure, would enable the cryptography method because the basic of encrypting require a non group algorithm, because is used has a key for encrypt the message.

As to claim 24, Seheidt et al. as modified teaches wherein the algebraic structure is not associative (see Seheidt et al., column 4, lines 57-60).

As to claim 25, Seheidt et al. as modified teaches wherein the algebraic structure is not commutative (see Seheidt et al., column 4, lines 57-60).

As to claim 26, Seheidt et al. as modified teaches the algebraic

structure is not commutative (see Seheidt et al., column 4, lines 57-60).

As to claim 28, Seheidt et al. as modified teaches wherein the method uses a near ring (see Anshel et al., column 1, lines 31-35; column 7, line 16).

12. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Scheidt et al. (U.S. patent 6,266,417) as applied in claims 2-3, 5-6, 8, 14-16, and 19-21 above, and further in view of Anshel et al (U.S. patent 5,440,640).

As to claim 27, Seheidt et al. '173 as modified does not teach wherein the arithmetic is a crossed inverse quasigroup.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches wherein the arithmetic is a crossed inverse quasigroup (see column 2, lines 46-61).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, as modified, to include wherein the arithmetic is a crossed inverse quasigroup.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, as modified, by the teaching of Scheidt et al. '417, because wherein the arithmetic is

a crossed inverse quasigroup, would enable the cryptography method because the crossed inverse quasigroup is a mathematical structure (same arithmetic).

13. Claims 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Scheidt et al. (U.S. patent 6,266,417) as applied in claims 2-3, 5-6, 8, 14-16, and 19-21 above, and further in view of Akatsu (U.S. patent 5,982,890).

As to claim 29, Seheidt et al. '173 teaches encrypt a message using a non-associative arithmetic (see column4, lines 57-60).

Seheidt et al. '173 does not teach send the encrypted message.

Scheidt et al. '417, teaches cryptographic communication process and apparatus (see abstract), in which he teaches send the encrypted message (see column 1, lines 32-35).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 , to include send the encrypted message.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 by the teaching of Scheidt et al. '417, because send the encrypted message, would enable the method to send the message automatically when the encryption is finish, because the computer has the instruction stored.

Seheidt et al. '173 as modified does not teach an apparatus comprising a program stored on a computer readable media including instructions.

Akatsu, teaches method and system for detecting fraudulent data update (see abstract), in which he teaches an apparatus comprising a program stored on a computer readable media including instructions (see column 4, lines 32-64).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173, as modified, to include an apparatus comprising a program stored on a computer readable media including instructions.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 as modified, by the teaching of Akutsu, because an apparatus comprising a program stored on a computer readable media including instructions, would enable the cryptography method to operated automatically because the program know what the computer have to do, when the user want to encrypt a message.

As to claim 30, Seheidt et al. '173 as modified teaches wherein the arithmetic includes a non-trivial crossed inverse quasigroup (see Scheidt et al. '417, column 2, lines 46-53).

As to claim 31, Seheidt et al. '173 as modified teaches wherein the arithmetic is one which is based on a multiplication table which is expressed as a rule (see Scheidt et al. '417, column 2, lines 62-64; column 9, lines 28-35).

As to claim 32, Seheidt et al. '173 as modified teaches an apparatus further comprising adding a random seed to the arithmetic (see Scheidt et al. '417, column 9, lines 31-35).

14. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seheidt et al. (U.S. patent 5,787,173) in view of Scheidt et al. (U.S. patent 6,266,417) further in view of Akatsu (U.S. patent 5,982,890) as applied in claims 29-32 above, and further in view of Hellman et al., (U.S. patent 4,218,582).

As to claim 33, Seheidt et al. '173 as modified, does not teach an apparatus further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption.

Hellman et al., teaches exponentiation cryptographic apparatus and method (see abstract), in which he teaches an apparatus further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption (see column 10, lines 61-64).

Therefore, it would have been obvious to a person having ordinary

skill in the art at the time the invention was made to have modified Seheidt et al. '173 , as modified, to include an apparatus further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Seheidt et al. '173 as modified, by the teaching of Hellman et al., because an apparatus further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption, would enable the method to have space to the second encryption because is n x n (latin square) that duplicate the number.

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Belix M. Ortiz whose telephone number is 703-305-7605. The examiner can normally be reached on moday-friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 703-305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

bmo

March 18, 2004

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100